DEPARTMENT OF THE NAVY
NAVAL HOSPITAL
BOX 788250
MARINE CORPS AIR GROUND COMBAT CENTER
TWENTYNINE PALMS, CALIFORNIA 92278-8250

IN REPLY REFER TO:
NAVHOSP29PALMSINST 5230.2
Code 0103
17 June 1997

NAVAL HOSPITAL TWENTYNINE PALMS INSTRUCTION 5230.2

From: Commanding Officer

Subj: ELECTRONIC MAIL (E-MAIL) AND INTERNET USE ABOARD NAVAL HOSPITAL TWENTYNINE PALMS AND MCAGCC

Ref: (a) SECNAVINST 5216.5D
(b) BUMED INSTRUCTION 5230.4A
(c) COMBAT CENTER ORDER 5230.1
(d) MHSS AIS SECURITY BULLETIN “Acceptable Internet Use Guidelines” 97-001

Encl: (l) Electronic Mail (E-MAIL) and Freedom of Information/Privacy Act Guidance

1. Purpose. To provide policy regarding permissible and prohibited use of Electronic Mail (E-Mail) and the Internet for Naval Hospital Twentynine Palms staff using government equipment. Violations of the prohibited activities listed in paragraphs 4.b.(3) and 4.b.(4) below, may result in administrative and/or disciplinary action.

2. Scope. This instruction applies to all personnel who have authorized access to the NAVHOSP29PALMS and MCAGCC network.

3. Definitions

a. Electronic Mail. Electronic mail (E-Mail) is an authorized means of communication that uses computer-to-computer data transfer technology, normally in the form of textual messages. It also has the ability to carry a “payload” in the form of an attached file. That payload can be any type of file (i.e., text, graphics, programs, etc.).

b. Individual E-Mail. Individual E-Mail is a message or file transmitted to or from an individual’s personal mailbox containing informal information that does not commit or direct an organization. The purpose of individual E-Mail is to facilitate the direct exchange of information in the same manner as the telephone, voice mail, or FAX machine.

c. Individual Mailbox. Individual Mailbox (IMB) is the E-Mail address of an individual to and/or from which individual E-Mail is sent. In accordance with established security procedures, access to this mailbox is only by the individual to whom it is assigned.

d. Internet. The Internet is a global digital infrastructure that connects millions of computers and tens of millions of people globally.

e. World Wide Web. World Wide Web (WWW) is a mechanism that simplifies the retrieval and display of information on the Internet.

f. Non-Secure Internet Protocol Router Network. Non-Secure Internet Protocol Router Network (NIPRNET) is a global digital infrastructure that provides a world wide network for the DoD/DON/USN/USMC and a path to the Internet.

4. Guidelines

a. E-Mail

(1) Per reference (a), E-Mail is intended primarily for official Government business only.

(2) Personal E-Mail sent or received via the Internet is authorized as long as:

(a) DoD maintains connectivity between NIPRNET and the Internet.

(b) It does not violate the criteria established in paragraph 4.b.(4) below, for Internet access.

b. Internet

(1) Use of the Internet will be in accordance with reference (d). Due to current MCAGCC and Naval Hospital bandwidth limitations and network degradation, WWW broadcast media using “push technology” (i.e., Pointcast) is restricted.

(2) Internet services can be used when work related and determined to be in the best interests of the Federal Government, the Navy, and the Marine Corps. Examples are:

(a) Obtain information to support missions.

(b) Obtain information that enhances the professional skills of military/civil service personnel.

(c) Improve professional or personal skills as part of a formal academic education or military/civilian professional development program.

(3) Government computers may be used to access the Internet for incidental personal purposes such as Internet searches and communications as long as such use:

(a) Does not adversely affect the performance of duties.

(b) Serves a legitimate professional interest such as enhancing personal skills or obtaining information.

(c) Does not overburden Marine Corps computing resources or communication systems.

(d) Not used for purposes that adversely reflect upon the DoD/DON/USN/USMC.

(4) Use of government resources to connect to the Internet for purposes other than those described in paragraphs 4b(2) and 4b(3) above, is prohibited. Examples of prohibited use include, but are not limited to the following:

(a) Illegal, fraudulent or malicious activities.

(b) Partisan political activity, political or religious lobbying or advocacy on behalf or organizations having affiliation with DoD/DON/USN/USMC.

(c) Activities whose purposes are for personal or commercial financial gain, to include chain letters.

(d) Unauthorized fund raising.

(e) Accessing, storing, processing, displaying, or distributing offensive or obscene material such as pornography and hate literature.

(f) Obtaining, transporting, installing, or using software obtained in violation of the appropriate vendors patent, copyright, trade secret or license statement (including shareware).

(g) Participation in Chat Rooms for uses other than those outlined in paragraphs 4b(2) and 4b(3).

(h) Using Marine Corps internet resources as an Internet Service Provider (ISP) for uses other than those outlined in paragraphs 4b(2) and 4b(3) above.

c. Access

(1) The Departmental/Divisional Terminal Area Security Officer (TASO) will forward all requests for E-Mail, Internet and WWW access to the Management Information Department (MID).

(a) E-Mail. Submit request for an account with the individual's rank, full name (LAST, FIRST, MI), position/title, phone number, and Directorate/Department/Division assigned.

(b) Internet/WWW. Submit individual's E-Mail address and service request.

4. Action

a. Directors, Department Heads, Division Officers

(1) Ensure that these policy guidelines are followed.

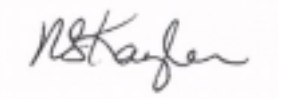
(2) Control and monitor access and usage within their respective Directorates, Departments, Divisions.

b. Head, Management Information Department

(1) Monitor the proper use of E-Mail and Internet access, as well as network resources.

(2) Restrict access to E-Mail and Internet, when required (i.e., misuse investigations, decreased network resources, etc.).

(3) Provide guidance and technical assistance on appropriate E-Mail and Internet access procedures and policies.



R. S. KAYLER

Distribution:
List A

ELECTRONIC MAIL (E-Mail) AND FREEDOM OF INFORMATION/PRIVACY ACT GUIDANCE

Users of the E-Mail system should be aware that this method of communication is not exempt from the Freedom of Information Act (FOIA),5 U.S.C. section 552 (1982 & Supp. IV 1986) or Privacy Act, 5 U.S.C. section 552a (1982 & Supp. IV 1986). Problems may arise due to ease and informality of the system, coupled with a permanence not readily apparent.

The E-Mail system aids rapid transmission of information among commands. The user accesses the system via an individualized password and may then send or receive messages through a centralized computer network. Incoming messages are stored in a "host computer" that is linked by the Medical Open Architecture communications network or a modem to the user's personal computer. After reading messages, the recipient may delete or store the messages on the host computer hard disk, on his or her own computer, and/or in printout form.

FOIA provides a person a right to access to all information maintained by Federal agencies, unless exempted by the statute. FOIA applies to information stored in any form, including paper, ADP storage media, and computer printouts. Thus, E-Mail transmissions are subject to FOIA from the moment they are created until they no longer exist. Hard copies of E-Mail messages also fall under FOIA.

The Electronic Communications Privacy Act of 1986 authorizes employers to review the electronic mail of employees who utilize corporate systems. Commanding Officers and Officers-in-Charge should annually publish a notification to their staff that electronic mail is subject to review by system administrators. They should then direct their local system administrators to periodically review the content of electronic mail within the command to ensure the system is not being utilized for illegal or inappropriate purposes.

The Privacy Act provides individuals a right to access the records pertaining to themselves. If electronic mail is utilized to store records pertaining to individuals, or if electronic correspondence is filed using personal identifying information in the title (e.g., an individuals name, social security number, or personal identifier) then the subject of the electronic mail must be notified before release of the correspondence is authorized to a third party.

An important aspect of any communications system is security. All E-Mail users should ensure that access to the system is limited to those with authorization. Unauthorized disclosures may violate the Privacy Act or waive otherwise applicable FOIA exemptions. In those instances where disclosure of E-Mail communications is not desired, the following procedures are recommended:

1. Promptly delete E-Mail messages you do not desire to retain. Remember the E-Mail stays in the E-Mail folder until it is affirmatively deleted. Reading E-Mail will not delete it. Additionally, E-Mail messages will be part of the permanent back up archive if the messages are not deleted the same day.

2. Do not retain hard copies of E-Mail. Also be aware that filing messages by an individual's name or personal identifier may bring them within the purview of the Privacy Act.

3. When communicating sensitive information, consider using the telephone in lieu of E-Mail. Conversations are not subject to FOIA or the Privacy Act, although notes taken during a conversation may be.

In summary, when information transmitted by E-Mail is retained, in any form, it should be treated as any other Official Government record.